添付資料

【今月の呼びかけ】

「 あなたの銀行口座も狙われている！？ 」
― SpyEye（スパイアイ）ウイルスに注意！ ―

2011 年 6 月から 7 月にかけて、インターネットバンキングでの不正利用事件が発生しています。警察に約 10 の金融機関から被害相談や届出が出されていると報道されるなど、事態の深刻さを受け、IPA でも 8 月に緊急対策情報※1 として注意喚起を行いました。

この不正利用事件は、「SpyEye（スパイアイ）」というウイルスの感染被害で起こった可能性が考えられます。それは、SpyEye ウイルスに、日本の銀行を不正利用する機能が含まれていたためです。

IPA では、SpyEye の一種（v1.3.45）を入手し、解析を実施中です。今のところ全ての解析を終えていませんが、ここでは、現時点で判明している解析結果を基に、SpyEye とはどのようなウイルスで、感染するとどのような動作をするのかを示すとともに、被害に遭わないための対策を紹介します。

※1　IPA-「国内のインターネットバンキングで不正アクセスが相次いでいる問題について」

http://www.ipa.go.jp/security/topics/alert20110803.html

（1）SpyEye とは？

SpyEye とは、本来ウイルスを作成するツールの名称ですが、このツールから作成されたウイルスも SpyEye と呼ばれるため、ここでは、作成されたウイルス自体を指すことにします。

SpyEye は、こうしたツールから簡単に作成することができ、また、少しずつ機能の異なる SpyEye を簡単に作成できるため、多くの亜種が存在しています。

図 1-1：ウイルス作成者がツールを使ってウイルスを作り出すイメージ図

【i】SpyEye の出現

SpyEye は、インターネットバンキングで使われる ID とパスワードの窃取を目的としたウイルスです。最初の出現は、2009 年の終わり頃から 2010 年初めにロシアのアンダーグラウンドサイト※2 からと言われています。

それまで、インターネットバンキングの ID とパスワードの窃取を目的としたウイルスは、Zeus（ゼウス）と呼ばれるウイルスを作成するツールから作成されたウイルス（Zeus、Zbot）が主立ったものでした。SpyEye は、この Zeus を基に作られたものと考えられています。

※2　アンダーグラウンドサイト：インターネットを通じて、違法行為や犯罪行為の勧誘や依頼を受けるウェブサイト。

【ii】感染後の動作

今回の解析から、SpyEye の感染後の動作として次の 2 点を確認しました。

- 利用者が閲覧中のウェブサイトで入力した ID とパスワードを窃取
- 窃取した情報をインターネット経由でウイルス作成者が管理しているサーバーに送信

SpyEye がパソコンに感染すると、利用者が閲覧しているインターネットバンキングなどのウェブページで ID とパスワードの情報を窃取し、インターネットを通じてボット※3 に感染したパソコンを操作する特定のサーバーに情報を送信します。これは、SpyEye がボットネット※4 機能を有していることを示しています。

ボットネット機能を使えば、ウイルス作成者がインターネットを通じて感染させた SpyEye を新しいウイルスに置き換えることができます。ウイルス対策ソフトで検知できない新種ウイルスに置き換え続けることで、より見つかりにくく、長い期間感染させて必要な情報を窃取できるため、利用者にとって重大な脅威となるウイルスといえます。

※3　ボット（bot）：ボットとはウイルスの一種で、ボットに感染したパソコンは、インターネットを通じて外部から操られてしまいます。

※4　ボットネット（botnet）：ボットネットとは、ボット（bot）に感染したパソコンとそれを操作するサーバーからなるネットワークのこと。

（ご参考）

ボット対策のしおり（IPA）

http://www.ipa.go.jp/security/antivirus/documents/3_bot_v6_2.pdf

（2）SpyEye の感染手口

SpyEye の主な感染手口として、次の 2 つが考えられます。

【i】ウェブサイトからダウンロードさせる

ウェブサイトを閲覧した際に、パソコン利用者の意図に関わらず、ウイルスなどの不正プログラムをパソコンにダウンロードさせる手法で「“ドライブ・バイ・ダウンロード”攻撃」と呼ばれます。"ドライブ・バイ・ダウンロード"攻撃では、主に利用者のパソコンの OS やアプリケーションなどの脆弱（ぜいじゃく）性が悪用されます。

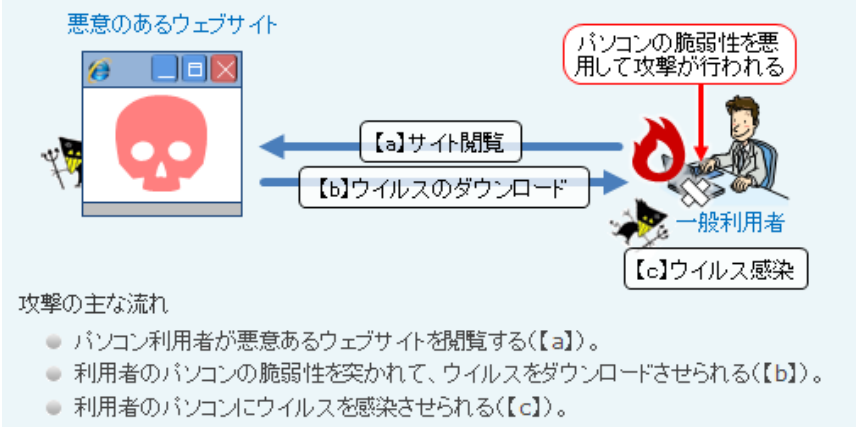

図 1-2：”ドライブ・バイ・ダウンロード”攻撃のイメージ

ウイルスを感染させる際の常とう手段となっている”ドライブ・バイ・ダウンロード”攻撃ですが、SpyEye を感染させる手口にも使われています。

（ご参考）

「ウェブサイトを閲覧しただけでウイルスに感染させられる"ドライブ・バイ・ダウンロード"攻撃に注意しましょう！」（IPA）

http://www.ipa.go.jp/security/txt/2010/12outline.html

【ii】メールで送りつける

ウイルスが感染している添付ファイル付きメールを送り、添付ファイルを開かせて感染させる手口も既に常とう手段となっています。この手口では、タイトルや添付ファイル名、メール本文や送信元詐称などによって、なんとかしてメールの添付ファイルを開かせようとします。

最近では、関係機関や関係者を装い、組織や個人を絞ってウイルスが感染している添付ファイルを送りつける「標的型攻撃」メールも多くなっています。

（ご参考）

災害情報を装った日本語のウイルスメールについて（IPA）

http://www.ipa.go.jp/security/topics/alert20110404.html

（3）対策

【i】OS やアプリケーションソフトの脆弱性を解消する

Windows などの OS や、アプリケーションの脆弱性を解消しておくことが重要です。**一般的に利用者の多いアプリケーションは狙われやすい傾向にあるため、脆弱性を解消して、常に最新の状態で使用してください。IPA では利用者のパソコンにインストールされているソフトウェア製品のバージョンが最新であるかを、簡単な操作で確認するツール「MyJVN バージョンチェッカ」を公開しています。なお、8 月 18 日から、サーバーに導入しているソフトウェアのバージョン確認や、Windows7（64bit 版）にも対応しました。**

（ご参考）

MyJVN バージョンチェッカ（IPA）

http://jvndb.jvn.jp/apis/myjvn/vccheck.html

サーバーソフトウェアもチェック可能となった「MyJVN バージョンチェッカ」

～システム管理者は脆弱（ぜいじゃく）性対策がなされたサーバーソフトウェアの使用を～

http://www.ipa.go.jp/about/press/20110818.html

【ii】ウイルス対策ソフトでウイルスの侵入を防止する

ウイルス対策ソフトを導入し、ウイルス定義ファイルを最新に保つことで、ウイルスの侵入阻止や、侵入したウイルスの駆除ができます。**近年のウイルスは、パソコンの画面の見た目では感染していることが分からないものが多いため、ウイルスの発見と駆除にはウイルス対策ソフトが必須です。**

【iii】簡単にメールの添付ファイルを開かない

普段やり取りがない送信者からのメールが届いたら、不用意に開いたり、メール本文に書いてあるリンクを安易にクリックしたりしないでください。可能であれば送信者と連絡を取り、本当にその送信者が送ったメールなのかを確認してください。ただし、確認をする際は、メールの中に書かれている連絡先には連絡をせず、出来る限り自分で連絡先を調べて電話で確認することを勧めます。

添付ファイルがあるメールであれば、普段やり取りのある送信者からのメールでも用心し、少しでも不自然だと思うメールであれば、相手に確認を取るか、メールそのものを読まずに削除することが最善策です。

【iv】ID やパスワードを使い回さない

SpyEye は、インターネットバンキングで使われる ID とパスワードの窃取を目的としています。**もし、感染被害に遭い ID とパスワードを窃取されてしまった場合、その ID やパスワードを他のウェブサイトでも使い回していると、そのウェブサイトのサービスでも連鎖的に不正利用の被害に遭う可能性があります。**

パスワードは、いつでも悪意ある者に狙われているという意識を持つべきです。また、下記のウェブページを参考にしてパスワードの適切な管理を心がけてください。

インターネットバンキングでは、その時だけ有効なパスワードを発行する「ワンタイムパスワード」というサービスを提供していることがあります。ID やパスワードを盗むウイルスに感染していても、一度きりのパスワードのため、仮に盗まれてもその後悪用されることはありませんので、このサービスの利用をお勧めします。

（ご参考）

「パスワード ぼくだけ知ってる たからもの」（IPA）

http://www.ipa.go.jp/security/txt/2011/06outline.html

【v】ウイルスに感染してしまった場合の対策

SpyEye に限らず、ウイルスに感染した疑いがある場合（動作が遅い、不自然な動きをする、出所不明なファイルを開いてしまったなど）は、まず、ウイルス定義ファイルが最新の状態になったウイルス対策ソフトで、パソコン内のウイルスチェックを行ってください。

SpyEye は、ウイルス作成者がいつでも新しい SpyEye に置き換えることができるため、ウイルス対策ソフトで発見されない場合があります。ウイルスチェックをしても見つからない、または駆除をしたにもかかわらず正常に動作していないと思われるのであれば、パソコンを購入した時の状態に戻す作業（初期化）を行ってください。

実際の作業方法は、パソコンに付属の取扱説明書に記載されている「購入時の状態に戻す」などの手順に沿って作業してください。なお、作業を行う前には、重要なデータのバックアップを忘れずに行ってください。また、バックアップしたデータは、パソコンに戻す前にウイルス対策ソフトでウイルスチェックし、ウイルスが含まれていないことを確認してください。

もし、インターネットバンキングの不正利用の被害に遭ってしまった場合は、当該銀行への問い合わせをしてください。多くの銀行では、ウェブサイトのトップページから問い合わせができるようになっています。さらに、ウイルスに感染していない、自分自身が管理している安全なパソコンから、インターネットバンキングで使用しているパスワードを変更してください。